Small Business Administration

Privacy Impact Assessment

For

Denver Finance Center System

08/2005

Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the Denver Finance Center Consolidated System. This document has been completed in accordance with the requirements of the E-Government Act of 2002.

MANAGEMENT CERTIFICATION – Please check the appropriate statement.

_____ The document is accepted.

_____ The document is accepted pending the changes noted.

_____ The document is not accepted.

_____**We** fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

_____	_____
System Manager	DATE
_____	_____
OCIO/Project Representative	DATE
_____	_____
Program/Office Head	DATE
_____	_____
OCIO	DATE
_____	_____
Senior Official for Privacy	DATE

Name of Project: Denver Finance Center System
Program Office: OCFO
Project's Unique ID:

A. CONTACT INFORMATION:

1. Who is the person completing this document?

Blake E. Hoing
Lead IT Specialist
OCFO/OFS Denver
(303) 844-5706
blake.hoing@sba.gov

2. Who is the system owner?

Tom Dumaresq
Chief Financial Officer
(202) 205-6449
tom.dumaresq@sba.gov

3. Who is the system manager for this system or application?

Blake E. Hoing
Lead IT Specialist
OCFO/OFS Denver
(303) 844-5706
blake.hoing@sba.gov

4. Who is the IT Security Manager who reviewed this document?

Ethel Matthews
Chief Information Security Officer
(202) 205-7173
ethel.matthews@sba.gov

5. Who is the Privacy Officer who reviewed this document?

Lisa Babcock
Chief, FOI/PA
(202) 401-8203
lisa.babcock@sba.gov

6. **Did the Agency's Senior Office for Privacy review this document?** Yes.

Delorice Ford
Agency Senior Privacy Official
delorice.ford@sba.gov
(202) 205-7340

7. **Who is the Reviewing Official?**

Delorice Ford
Agency Senior Privacy Official
delorice.ford@sba.gov
(202) 205-7340

B. SYSTEM APPLICATION/GENERAL INFORMATION:

1. **Does this system contain any information about individuals?** Yes.

   (a) Is this information identifiable to the individual? **Y**es.

   (b) Is the information about individual members of the public? Yes.

   (c) Is the information about employees? Yes

2. **What is the purpose of the system/application?**

The Treasury Disbursements sub system of the DFCCS maintains a register of all disbursements made, which includes employee, vendor, bank, and borrower information.

3. **What legal authority authorizes the purchase or development of this system/application?**

   15 U.S.C. § 634(b)(6), 44 U.S.C. § 3101. Public Law 85-536, 15 U.S.C. § 631 et seq. (Small Business Act, all provisions relating to loan programs); 44 U.S.C. § 3101 (Records Management by Federal Agencies); and Public Law 103-62 (Government Performance and Results Act). Public Law 85-699 as amended 15 U.S.C. §661 et seq. (Small Business Investment Act of 1958, all provisions relating to loan programs)

C. DATA in the SYSTEM:

1. **Generally describe the type of information to be used in the system and what categories of individuals are covered in the system?**

   The Treasury Disbursements sub system of the DFCCS maintains a register of all disbursements made, which includes employee, vendor, bank, and borrower information. Information maintained includes name, address, city, state, zip, loan Numbers, RTN's, Bank Account Numbers, Bank Account types.

2. **What are the sources of the information in the system?**

   (a) Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

The initial information is gathered from the individual, but for purposes of disbursement, the information is collected from various systems, including JAAMS, PIMS, and LAS.

(b) What Federal agencies are providing data for use in the system?

None.

(c) What Tribal, State and local agencies are providing data for use in the system?

None.

(d) From what other third party sources will data be collected?

None.

(e) What information will be collected from the employee and the public?

We do not collect information, we use what has been collected by Loan Officers, etc.

3. Accuracy, Timeliness, and Reliability

(a) How will data collected from sources other than SBA records be verified for accuracy?

N/A

(b) How will data be checked for completeness?

N/A

(c) Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

We use the information available to us. Maintaining the currency of that information is beyond our scope.

(d) Are the data elements described in detail and documented? If yes, what is the name of the document?

No. However, the initial collection point (Loan Officers, etc) may have more detailed documentation.

D. ATTRIBUTES OF THE DATA:

1. **Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

   Yes.

2. **Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

   No.

3. **Will the new data be placed in the individual's record?**

   No.

4. **Can the system make determinations about employees/public that would not be possible without the new data?**

   No.

5. **How will the new data be verified for relevance and accuracy?**

   N/A

6. **If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?**

   Sybase Access Controls as well as file level access controls. Agency Security Access Procedures – Data access is limited to those individuals with authorized use and only for specific screens as they pertain to the user's role/need.

7. **If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access?**

   N/A

8. **How will the data be retrieved?** Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Yes. Information can be retrieved by SSN, TIN, Name, Loan Number.

9. **What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?**

   Automated queries are done to evaluate the disbursement history, track down missing payments, and to process cancellation transactions on disbursements that are not actually cleared by the payee.

10. **What opportunities do individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses and how individuals can grant consent.)**

    We do not collect the information, we merely store what is provided to us.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1. **If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?**

   It is operated at one site only.

2. **What are the retention periods of data in this system?**

   As specified in SBA's Privacy Act Systems of Records, SBA 20 and SBA 21, In accordance with SBA Standard Operating Procedure 00 41 2, Item Nos. 50:04, 50:08, 50:09, 50:10, 50:11, 50:12, 50:13, 50:19, 50:22, 55:02, 70:09, 70:13, and appendices 17, 18 and 21.

3. **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

   As delineated in SBA's Privacy Act Systems of Records, SBA 20 and SBA 21. In accordance with SBA Standard Operating Procedure 00 41 2, Item Nos. 50:04, 50:08, 50:09, 50:10, 50:11, 50:12, 50:13, 50:19, 50:22, 55:02, 70:09, 70:13, and appendices 17, 18 and 21.

4. **Is the system using technologies in ways that the SBA has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

   No

5. **How does the use of this technology affect public/employee privacy?**

Information is used only in the course of the disbursements/cancellations cycle.

6. **Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.**

   No.

7. **What kinds of information are collected as a function of the monitoring of individuals?**

   N/A

8. **What controls will be used to prevent unauthorized monitoring?**

   Agency Security Roles and Procedures/Controls – Agency Security Access Procedures – Access is limited by controlled assignment of a responsibility profile to all users. Each responsibility comes with a pre-determined set of privileges, limiting data that may be viewed to those screens and reports that are within the duties and needs of the user

9. **Under which Privacy Act systems of records notice does the system operate? Provide number and name.**

   SBA's Privacy Act Systems of Records, SBA 20 and SBA 21

10. **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

    It is not being modified.

F. <u>ACCESS TO DATA:</u>

1. **Who will have access to the data in the system?**

   Users are within the Denver Finance Center.

2. **How is access to the data by a user determined?**

   There are technical controls to ensure that only authorized users have access, as well as managerial controls to ensure that users are authorized access. Annual recertifications and reconciliations ensure the quality of the security program.

3. **Will users have access to all data on the system or will the user's access be restricted? Explain.**

Users who have been duly authorized access to the system have full access. However, in place technical controls ensure that they have no ability to change any data.

4. **What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access?** (Please list processes and training materials)

   Access is limited via userid and password controls, and rights are assigned to groups within the Operating System. In addition, education of agency personnel regarding privacy act rules and prohibitions is both mandatory and ongoing. Agency network login procedures mandate a posted privacy notice be viewed and acknowledged prior to entry. In addition, we follow the principal of least access as the most appropriate and significant control.

5. **Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system**? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed?

   No.

6. **Do other systems share data or have access to the data in the system? If yes, explain.**

   The 1098 System for Cancellation of disbursements accesses these records to determine who a payment was made to, and how to cancel the disbursement.

7. **Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?**

   The System Manager is responsible for protecting the privacy rights of the public and employees.

8. **Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)?**

   No.

9. **How will the data be used by the other agency?**

   N/A

10. **Who is responsible for assuring proper use of the data?**

    The System Manager.

APPENDIX A
DECLARATION OF PRIVACY PRINCIPLES

The privacy principles set forth in this declaration are based on the ethical and legal obligations of the Small Business Administration to the public and are the responsibility of all SBA employees to recognize and treat their office as a public trust.

The obligation to protect client and partner privacy and to safeguard the information clients and partners entrust to us is a fundamental part of the SBA's mission to administer the law fairly and efficiently. Clients and partners have the right to expect that the information they provide will be safeguarded and used only in accordance with law. In recognition of these obligations, policies and procedures must clearly state who should have access to what information and for what purposes. In addition, appropriate limitations must be placed on the collection, use and dissemination of clients and partners' personal and financial information and sufficient technological and administrative measures must be implemented to ensure the security of SBA data systems, processes and facilities.

All SBA employees are required to exhibit individual performance that reflects a commitment to dealing with every client and partner fairly and honestly and to respect the clients and partners' right to feel secure that their personal information is protected. To promote and maintain clients and partners' confidence in the privacy, confidentiality and security protections provided by the SBA, the SBA will be guided by the following Privacy Principles:

Principle 1:	Protecting citizen, client and partner privacy and safeguarding confidential citizen, client and partner information is a public trust.
Principle 2:	No information will be collected or used with respect to citizens, clients and partners that is not necessary and relevant for legally mandated or authorized purposes.
Principle 3:	Information will be collected, to the greatest extent practicable, directly from the citizen, client or partner to whom it relates.
Principle 4:	Information about citizens, clients and partners collected from third parties will be verified to the greatest extent practicable with the citizens, clients and partners themselves before action is taken against them.
Principle 5:	Personally identifiable citizen, client or partner information will be used only for the purpose for which it was collected, unless other uses are specifically authorized or mandated by law.
Principle 6:	Personally identifiable citizen, client or partner information will be disposed of at the end of the retention period required by law or regulation.

Principle 7:	Citizen, client or partner information will be kept confidential and will not be discussed with, nor disclosed to, any person within or outside the SBA other than as authorized by law and in the performance of official duties.
Principle 8:	Browsing, or any unauthorized access of citizen, client or partner information by any SBA employee, constitutes a serious breach of the confidentiality of that information and will not be tolerated.
Principle 9:	Requirements governing the accuracy, reliability, completeness, and timeliness of citizen, client or partner information will be such as to ensure fair treatment of all clients and partners.
Principle 10:	The privacy rights of citizens, clients and partners will be respected at all times and every citizen, client and partner will be treated honestly, fairly, and respectfully.

The Declaration does not, in itself, create any legal rights for clients and partners, but it is intended to express the full and sincere commitment of the SBA and its employees to the laws which protect client and partner privacy rights and which provide redress for violations of those rights.

APPENDIX B
POLICY STATEMENT ON CITIZEN, CLIENT AND PARTNER PRIVACY RIGHTS

The SBA is fully committed to protecting the privacy rights of all citizens, clients and partners. Many of these rights are stated in law. However, the SBA recognizes that compliance with legal requirements alone is not enough. The SBA also recognizes its social responsibility which is implicit in the ethical relationship between the SBA and the citizen, client or partner. The components of this ethical relationship are honesty, integrity, fairness, and respect.

Among the most basic of a citizens, clients, or partners' privacy rights is an expectation that the SBA will keep personal and financial information confidential. Citizens, clients and partners also have the right to expect that the SBA will collect, maintain, use, and disseminate personally identifiable information and data only as authorized by law and as necessary to carry out agency responsibilities.

The SBA will safeguard the integrity and availability of citizens, clients and partners' personal and financial data and maintain fair information and record keeping practices to ensure equitable treatment of all citizens, clients and partners. SBA employees will perform their duties in a manner that will recognize and enhance individuals' rights of privacy and will ensure that their activities are consistent with law, regulations, and good administrative practice. In our record keeping practices, the SBA will respect the individual's exercise of his/her First Amendment rights in accordance with law.

As an advocate for privacy rights, the SBA takes very seriously its social responsibility to citizens, clients and partners to limit and control information usage as well as to protect public and official access. In light of this responsibility, the SBA is equally concerned with the ethical treatment of citizens, clients and partners as well as their legal and administrative rights.